REMARKS

Claims 1-46 are pending, with claims 1, 12, 20, 24, and 31 being independent. Claims 1, 12, 20, 24, and 31 have been amended. No new matter has been added. Reconsideration and allowance of the above-referenced application are respectfully requested.

Rejections Under 35 U.S.C. § 112

Claims 1-3, 6, 7, 9-14, 19-21, 23, 24, 27-35, 37, 39, 41 and 43 stand rejected under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the written description requirement. This contention is respectfully traversed.

Contrary to the Office's assertion, the original specification reasonably conveys to a person having ordinary skill in the art that the applicants had possession of the claimed subject matter at the time of filing of the application. For example, the application as filed describes that request messages (e.g., SYN requests) in the network traffic can be monitored. (See, e.g., page 4, lines 19-23, which states that "[t]he sending communications monitor 42 **monitors** the messages, including the **SYN requests**, passing through the interface device 20 (step 502). The sending flood detector 46 detects that a flood is occurring through that interface device 20 (step 504).")

Additionally, the application as filed describes that one example of SYN flood attack detection is by comparing the number of request messages with the network traffic, which includes a number of acknowledgment messages. (See, e.g., pages 6-7, which state that "In detecting a flood attack, a flood detector may employ one or more of several detection methods. For example, a flood detector can statistically analyze all communications through the interface device and determine that an

uncharacteristically large number of SYN requests are passing through the interface device. ... To detect an uncharacteristically large number of SYN requests, the **interface device can monitor the traffic through it to determine the normal level of traffic**. ... Still another example of a flood detection method is **comparing or correlating the number of SYN requests with corresponding final ACK messages** in order to determine the number of SYN requests that are **valid or invalid**. A 5-tuple caching technique can be used to handle packets that have already been seen. When the first SYN message comes in, the cache won't have an entry for the 5-tuple of that message (source IP, destination IP, IP protocol, source port, and destination port). When subsequent packets arrive, there will already be cached information."

Therefore, based on the original specification a person having ordinary skill in the art would understand that the applicants had possession of the claimed subject matter at the time of filing of the application. Thus, withdrawal of the rejections of claims 1-3, 6, 7, 9-14, 19-21, 23, 24, 27-35, 37, 39, 41 and 43 under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the written description requirement is respectfully requested.

Claims 1-3, 6, 7, 9-14, 19-21, 23, 24, 27-35, 37, 39, 41 and 43 stand rejected under 35 U.S.C. § 112, second paragraph as allegedly being indefinite. The term "tuple cache information" has been amended to recite "5-tuple packet information" to obviate these rejections.

The Office's statement that "it is unclear whether the process of monitoring network traffic, determining a number of valid request messages, comparing, communicating, etc. is with respect to brokers or the device associated with first and second points of a network" is respectfully traversed. Given the original specification and the plain reading of the claim

language, a personal of ordinary skill in the art would clearly understand what actions are performed by the brokers. For example, claim 1 recites "communicating the information … **to brokers** …; analyzing, **by the brokers**, …; and communicating **between the brokers** …."

Additionally, the Office's statement that "comparing current traffic information to the number of valid request messages … [of claim 1 is unclear]" is respectfully traversed. Amended claim 1 describes, among other features, a method that monitors network traffic (which includes the total number of request messages, whether valid or invalid); determines the number of valid and invalid request messages from the network traffic; compares the network traffic to the determined number of valid and invalid request messages to generate information about unwanted communications.

Thus, a person of ordinary skill in the art would clearly understand, given the original specification and the plain meaning of the claim language, what "comparing current network traffic to the number of valid and invalid request messages" is directed to. For example, in a SYN flood attack, the network traffic can have many invalid SYN request messages along with some valid SYN request messages. By comparing the number of valid SYN request messages to the network traffic (which includes the total number of SYN request messages and acknowledgment messages), a percentage of how much of the network traffic is used for valid SYN request can be determined. If this percentage is below a certain threshold, there is likely a SYN flood attack.

Therefore, based on the original specification a person having ordinary skill in the art would understand what the claimed subject matter is directed to. Thus, withdrawal of the rejections of claims 1-3, 6, 7, 9-14, 19-21, 23, 24, 27-35, 37,

39, 41 and 43 under 35 U.S.C. § 112, second paragraph as allegedly being indefinite is respectfully requested.

Rejections Under 35 U.S.C. § 101

Claims 31-35, 37, 39, 41 and 43 stand rejected under 35 U.S.C. § 101 for allegedly being directed to non-statutory subject matter. This contention is respectfully traversed. The Federal Circuit has long held that the **claimed invention as a whole** must be useful and accomplish a practical application; i.e., it must produce a "useful, concrete and tangible result." (State Street Bank & Trust Co. v. Signature Financial Group Inc., 149 F. 3d 1368, 47 USPQ2d 1596, 1601-02 (Fed. Cir. 1998).)

Claim 31 recites, among other features: "**monitor** network traffic; … **generate information** … about unwanted communications; **communicating the information** …" (emphases added.) Claim 31 generates information, communicates the generated information, and acts on it. The actions and operations are all tangible. Thus, claim 31, as a whole, is useful, performs operations that are tangible, and accomplishes a practical application by detecting unwanted communications (e.g., a SYN attack) in the network traffic. Therefore, withdrawal of the rejection of claim 31 under 35 U.S.C. § 101 is respectfully requested. Additionally, claims 32, 35, 37, 39, 41, and 43 depend from claim 31 or other statutory independent claims and their rejections should also be withdrawn for at least the reasons provided above.

Rejections Under 35 U.S.C. § 102

Claims 1-3, 6, 7, 9-14, 19-21, 23, 24, 27-35, 37, 39, 41 and 43 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Chen et al. (U.S. 2002/0103916 A1; hereinafter "Chen"). The claims have been amended to obviate these rejections.

For example, while the cited portions of Chen (page 6, [0078]-[0079]) disclose keeping the mean and standard deviation for a set of parameters (e.g., source and destination network addresses, protocols) in the network traffic, Chen fails to disclose caching the 5-tuple packet information for request messages in the network traffic. For example, the application as filed describes that "[a] 5-tuple caching technique can be used to handle packets that have already been seen. When the first SYN message comes in, the cache won't have an entry for the 5-tuple of that message (**source IP, destination IP, IP protocol, source port, and destination port**). When subsequent packets arrive, there will already be cached information."

Thus, Chen does not disclose each and every element and limitation of claim 1, and claim 1 should be in condition for allowance. Independent claims 12, 20, 24, and 31 have also been amended to include the limitation of caching of 5-tuple packet information for request messages in the network traffic. Therefore, independent claims 12, 20, 24, and 31 are also allowable for at least the reasons described above for claim 1. Claims 2-3, 6-7, 9-11, 13-14, 19, 21, 23, 27-30, 32, 35, 39, 41 and 43 depend generally from claims 1, 12, 20, 24, or 31, and there are allowable for at least the reasons provided above.

Concluding Comments

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as

specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicants ask that all claims be allowed. Please apply applicable charges or credits to Deposit Account No. 06 1050.

Respectfully submitted,

Date: 6/29/2007

Scott C. Harris
Reg. No. 32,030
Attorney for Intel Corporation

/BY
CHENG C. KO
REG. NO. 54,227

Fish & Richardson P.C.
PTO Customer No.: **20985**
(858) 678-5070 telephone
(858) 678-5099 facsimile

10750525.doc